An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2605150201

NCSC Advisory

Cisco: Cisco Catalyst SD-WAN Products

CVE-2026-20182

15th, May 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-20182

Published: 2026-05-14

Vendor: Cisco

Product: Cisco Catalyst SD-WAN Manager

CVSS Score[1]: 10

Products Affected

Product	Version
Cisco Catalyst SD-WAN Manager	20.1.12
Cisco Catalyst SD-WAN Manager	19.2.1
Cisco Catalyst SD-WAN Manager	18.4.4
Cisco Catalyst SD-WAN Manager	18.4.5
Cisco Catalyst SD-WAN Manager	20.1.1.1
Cisco Catalyst SD-WAN Manager	20.1.1
Cisco Catalyst SD-WAN Manager	19.2.099
Cisco Catalyst SD-WAN Manager	18.3.6
Cisco Catalyst SD-WAN Manager	18.3.7
Cisco Catalyst SD-WAN Manager	19.2.0
Cisco Catalyst SD-WAN Manager	19.1.0
Cisco Catalyst SD-WAN Manager	18.4.303
Cisco Catalyst SD-WAN Manager	19.2.098
Cisco Catalyst SD-WAN Manager	18.3.6.1
Cisco Catalyst SD-WAN Manager	18.2.0
Cisco Catalyst SD-WAN Manager	17.2.8
Cisco Catalyst SD-WAN Manager	18.3.3.1

[1] https://www.first.org/cvss/

Cisco Catalyst SD-WAN Manager	18.4.0
Cisco Catalyst SD-WAN Manager	18.3.1
Cisco Catalyst SD-WAN Manager	17.2.6
Cisco Catalyst SD-WAN Manager	17.2.9
Cisco Catalyst SD-WAN Manager	17.2.5
Cisco Catalyst SD-WAN Manager	18.4.0.1
Cisco Catalyst SD-WAN Manager	18.3.3
Cisco Catalyst SD-WAN Manager	18.3.0
Cisco Catalyst SD-WAN Manager	19.2.3
Cisco Catalyst SD-WAN Manager	18.4.501_ES
Cisco Catalyst SD-WAN Manager	20.1.2
Cisco Catalyst SD-WAN Manager	19.2.929
Cisco Catalyst SD-WAN Manager	19.2.31
Cisco Catalyst SD-WAN Manager	20.3.2
Cisco Catalyst SD-WAN Manager	19.2.4
Cisco Catalyst SD-WAN Manager	19.2.4.0.9
Cisco Catalyst SD-WAN Manager	20.1.3.1

Impact

A vulnerability in the peering authentication in Cisco Catalyst SD-WAN Controller, formerly SD-WAN vSmart, and Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, could allow an unauthenticated, remote attacker to bypass authentication and obtain administrative privileges on an affected system.

This vulnerability exists because the peering authentication mechanism in an affected system is not working properly. An attacker could exploit this vulnerability by sending crafted requests to the affected system. A successful exploit could allow the attacker to log in to an affected Cisco Catalyst SD-WAN Controller as an internal, high-privileged, non-root user account. Using this account, the attacker could access NETCONF, which would then allow the attacker to manipulate network configuration for the SD-WAN fabric.

Common Weakness Enumeration (CWE)[2]: CWE-287: Improper Authentication

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Cisco.

- https://nvd.nist.gov/vuln/detail/CVE-2026-20182
- https://www.cve.org/CVERecord?id=CVE-2026-20182
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-20182

[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog